


PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

# Rapport de certification ANSSI-CC-2011/14

# TrustyTime v2.1.5

*Paris, le 23 juin 2011*

*Le directeur général de l'agence nationale*
*de la sécurité des systèmes d'information*

Patrick Pailloux
[ORIGINAL SIGNE]



# Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.anssi@ssi.gouv.fr



| |
|---|
| *Référence du rapport de certification*<br>**ANSSI-CC-2011/14** |
| *Nom du produit*<br>**TrustyTime v2.1.5** |
| *Référence/version du produit*<br>**Version 2.1.5** |
| *Conformité à un profil de protection*<br>**Néant** |
| *Critères d'évaluation et version*<br>**Critères Communs version 3.1 révision 2** |
| *Niveau d'évaluation*<br>**EAL 3 augmenté**<br>**ALC_FLR.3** |
| *Développeur(s)*<br>**C.S.**<br>**22 avenue Galilée, 92350 Le Plessis-Robinson, France** |
| *Commanditaire*<br>**C.S.**<br>**22 avenue Galilée, 92350 Le Plessis-Robinson, France** |
| *Centre d'évaluation*<br>**Oppida**<br>**4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny le Bretonneux, France**<br>**Tél : +33 (0)1 30 14 19 00, mél : cesti@oppida.fr** |
| *Accords de reconnaissance applicables*<br>**CCRA**  **SOG-IS**  |

# Préface

## La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.



# Table des matières

# 1. Le produit

## 1.1. Présentation du produit

Le produit évalué est « TrustyTime v2.1.5 » développé par la société C.S.

Le produit TrustyTime est un système d'horodatage permettant d'émettre des jetons d'horodatage fiables. Ces jetons correspondent à l'association signée d'un condensé de document (obtenu par application d'une fonction de hachage sur le document à horodater), de la date et heure de l'horloge interne d'une unité d'horodatage, de la référence non ambiguë du certificat d'unité d'horodatage, et de la politique d'horodatage utilisée. Les jetons d'horodatage interviennent dans la construction de preuves de l'existence ou de l'antériorité d'un événement ou d'une transaction, de la possession ou de la validité de l'engagement d'un signataire à un instant donné.

TrustyTime permet de mettre en œuvre une ou plusieurs unités d'horodatage, identifiables par un nom donné par une autorité de certification. En conséquence, une unité d'horodatage n'existe pas en tant que telle avant qu'un certificat obtenu auprès d'une autorité de certification et permettant cette identification ne soit présent dans le système. Par ailleurs, pour représenter l'ensemble des informations permettant de définir une unité d'horodatage, les notions de contextes d'horodatage non opérationnels et opérationnels sont introduites.

Un contexte d'horodatage non opérationnel est défini comme l'ensemble des informations suivantes :

- l'identification de l'horloge interne utilisée pour obtenir la valeur du temps insérée dans le jeton d'horodatage ;
- la précision garantie pour la valeur du temps contenue dans le jeton d'horodatage par rapport au temps UTC (temps universel coordonné) ;
- la valeur de la bi-clé (et l'identifiant de l'algorithme à clé publique) pour la création et la vérification de la signature de jetons d'horodatage ;
- la durée d'utilisation de la clé privée qui a été définie à la création du contexte non opérationnel ;
- la ou les références des politiques d'horodatage supportées ;
- les identifiants des algorithmes de hachage pour chaque politique d'horodatage.

Un contexte d'horodatage opérationnel regroupe les informations d'un contexte d'horodatage non opérationnel, ainsi que les informations suivantes :

- la durée de vie effective de la clé privée du contexte qui est déterminée lors de l'import du certificat ;
- le certificat d'unité d'horodatage obtenu auprès d'une autorité de certification.

TrustyTime est un système d'horodatage fournissant également des fonctionnalités qui ne font pas partie de la TOE (*Target of evaluation* – Cible d'évaluation) : l'archivage et la conservation sur le long terme de la valeur probante des jetons d'horodatage délivrés.

## 1.2. Description du produit

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

### *1.2.1. Identification du produit*

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

La version certifiée du produit est identifiable par le nom des fichiers livrés (.jar), consignés dans le répertoire « applications » :
- tts-admin-<version>.jar ;
- tts-admin-server-<version>.jar ;
- tts-init-<version>.jar ;
- tts-server-<version>.jar ;
- tts-ta-proxy-<version>.jar (proxy d'archivage) ;

et par le fichier tts-proxy-<version>.war (proxy d'horodatage) consigné dans le répertoire « webapp ».
Ces références se retrouvent dans le bordereau de livraison accompagnant le produit.

Les versions des composants applicatifs sont aussi affichables par les commandes suivantes :

| Composants applicatifs | Commandes | Version |
|---|---|---|
| TTS-ADMIN | `Lunash:> sp tts-admin -version` | 2.1.5 |
| TTS-ADMIN-SERVER | `Lunash:> sp tts-admin-server -version` | 2.1.5 |
| TTS-INIT | `Lunash:> sp tts-init version` | 2.1.5 |
| TTS-SERVER | `Lunash:> sp tts-server -version` | 2.1.5 |
| TTS-TA-PROXY | `Lunash:> sp tts-ta-proxy -version` | 2.1.5 |
| TTS-PROXY | La version est consultable dans le fichier de log du proxy (par défaut « tts-proxy.log »). A chaque démarrage du proxy, la ligne suivante est inscrite dans le fichier : `......... tts-proxy (ver. 2.1.2) - started` | |

### *1.2.2. Services de sécurité*

Les principaux services de sécurité fournis par le produit sont :
- la génération de jetons d'horodatage ;
- la gestion des contextes d'horodatage ;
- la gestion des clés cryptographiques ;
- l'arrêt (temporaire ou définitif) d'une unité d'horodatage ;
- la gestion de la politique d'horodatage par défaut ;
- le suivi de la dérive des horloges internes d'unité d'horodatage et leur synchronisation avec l'UTC ;
- l'authentification des administrateurs de la TOE ;
- l'enregistrement des événements d'audit (en base de données) et la génération des alertes ;
- la consultation des journaux d'audit.

### 1.2.3. Architecture

Le produit TrustyTime est constitué d'une architecture logicielle divisée en cinq modules principaux :

- un module d'initialisation et de configuration de la TOE (Init) ;
- un module client pour lancer les commandes d'administration ;
- un module serveur de traitement des commandes d'administration sur le serveur d'horodatage ;
- un module serveur d'horodatage TCP/IP accessible aux utilisateurs du service ;
- un module proxy HTTP(S) redirigeant les demandes de jetons au serveur d'horodatage TCP/IP.

Cette architecture peut être représentée sous la forme suivante :

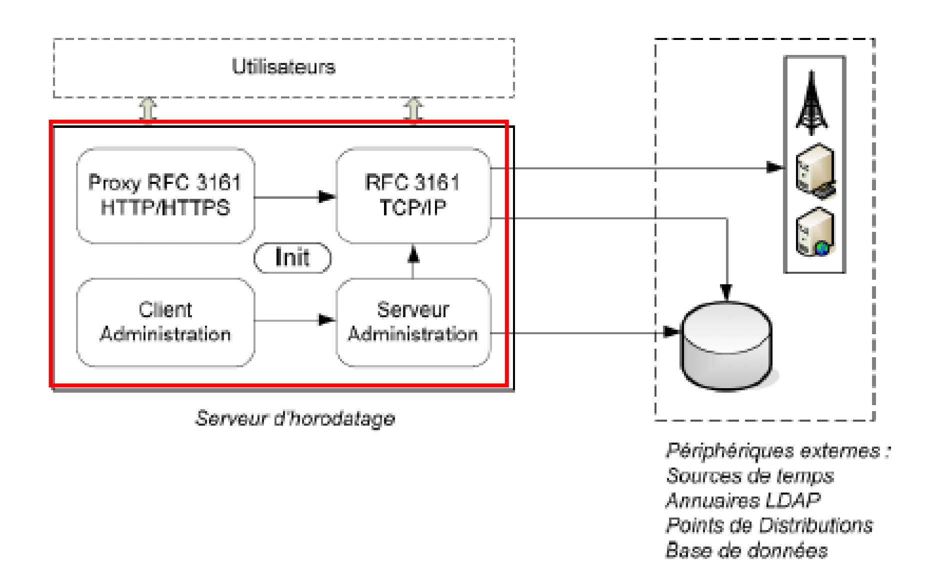



**Figure 1 - Architecture de la TOE**

### 1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :

- le développement et la livraison du produit sont réalisés par C.S. ;
- l'installation, l'administration et l'utilisation du produit correspondent au déploiement du produit par le client.

Le produit a été développé sur le site suivant :

**C.S.**

22 avenue Galilée
92350 Le Plessis-Robinson
France



Pour l'évaluation, l'évaluateur a considéré comme :

- administrateurs de la TOE les rôles suivants :
  - <u>administrateur de sécurité</u> : son rôle est de définir la politique d'horodatage par défaut, d'initialiser les unités d'horodatage, et de les remettre en route en cas d'arrêt automatique lorsqu'un redémarrage automatique n'est pas possible pour des raisons de sécurité ;
  - <u>auditeur</u> : son rôle est de définir les événements à tracer et d'analyser les événements d'audit concernant l'administration des unités d'horodatage et les synchronisations des horloges internes ;
- utilisateurs de la TOE les rôles suivants :
  - <u>opérateur</u> : son rôle est d'assurer le bon fonctionnement du système TrustyTime tant que les conditions de sécurité restent réunies ;
  - <u>superviseur</u> : son rôle est de vérifier le bon fonctionnement du système TrustyTime ;
  - <u>utilisateur</u> : son rôle est de soumettre des requêtes contenant les condensés de documents à horodater et l'identifiant de la fonction de hachage utilisée pour obtenir le condensé. Il doit également vérifier la validité du jeton d'horodatage délivré et s'assurer que le certificat d'unité d'horodatage correspondant est en cours de validité et n'a pas été révoqué.

### *1.2.5. Configuration évaluée*

La plateforme de tests mise en œuvre par le CESTI correspond à la configuration suivante :

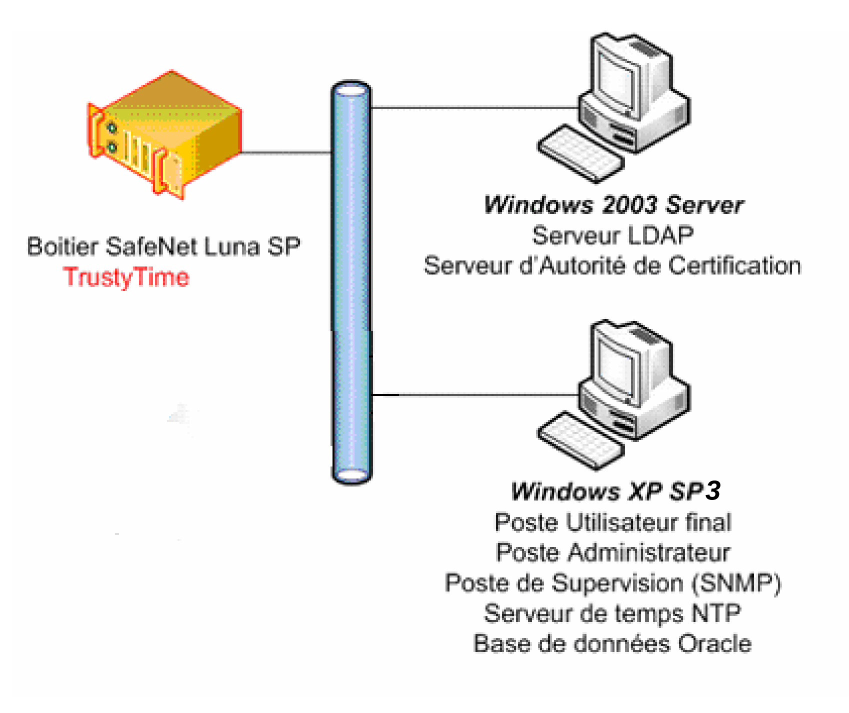



**Figure 2 - Plateforme de tests**

La plateforme d'évaluation est composée des équipements matériels et logiciels suivants :

- un boitier HSM SafeNet Luna SP v4.1.0-9 (firmware 4.6.1) hébergeant la TOE en version 2.1.5 ;

- un poste Windows XP SP3, où sont installés :
  - les clients logiciels SafeNet permettant d'accéder à la console d'administration et d'échanger des fichiers ;
  - un serveur de temps NTP (*Network Time Protocol* – Protocole d'heure réseau) ;
  - un collecteur d'alertes SNMP (*Simple network management protocol* – Protocole simple de gestion réseau) TrapReceiver v6.42 ;
  - l'utilitaire SQuirrel SQL v2.6.9 permettant d'accéder à la base de données Oracle 10g locale ;
- une machine virtuelle Windows 2003 Serveur offrant les services de serveur LDAP (*Lightweight Directory Access Protocol* – Protocole d'accès aux annuaires léger), d'autorité de certification et de point de distribution de listes de révocation ;
- un environnement JRE 1.5.07 et un serveur Apache Tomcat 5.5.16.

# 2. L'évaluation

## 2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 2** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

## 2.2. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 31 mai 2011, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

## 2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques selon les référentiels techniques [REF-CRY], [REF-KEY] et [REF-AUT] de l'ANSSI n'a pas été réalisée. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilités de conception et de construction pour le niveau AVA_VAN visé.

## 2.4. Analyse du générateur d'aléas

Le produit ne comporte pas de générateur d'aléas entrant dans le périmètre d'évaluation.

# 3. La certification

## 3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que le produit « TrustyTime v2.1.5 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 3 augmenté.

## 3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- (OE.LOCAL_ADMIN et OE.PROTECTION PHYSIQUE) l'administration de la TOE doit être effectuée localement, dans un environnement sécurisé à accès contrôlé et limité aux seules personnes autorisées ;

- (OE.RESEAU) le réseau sur lequel est connecté la TOE doit être déployé, configuré et administré conformément à une politique d'interconnexion de réseau assurant le filtrage des flux entrants et doit être protégé contre les attaques par déni de service ;

- (OE.ADMIN) les administrateurs de sécurité et les auditeurs doivent être formés aux tâches qu'ils ont à réaliser sur la TOE ;

- (OE.AUTORITE_HORODATAGE) l'autorité d'horodatage responsable du service d'horodatage fourni par la TOE doit appliquer les règles définies par les politiques d'horodatage spécifiées dans les contextes d'horodatage ;

- (OE.AUTORITE_CERT) les autorités de certification délivrant les certificats des unités d'horodatage doivent mettre en œuvre des pratiques, conformément à une politique de certification approuvée par l'autorité d'horodatage, couvrant les activités relatives à la délivrance et à la révocation de ces certificats ;

- (OE.SUPERVISION) le superviseur doit pouvoir consulter à distance l'état opérationnel du système d'horodatage ;

- (OE.IMPORT_CERTIFICAT) l'administrateur de sécurité doit vérifier, lors de l'import du certificat d'unité d'horodatage, qu'il provient bien d'une autorité de certification habilitée à délivrer des certificats pour un contexte donné ;



- le poste de supervision, le serveur de base de données, les serveurs de temps NTP et les points de distribution des listes de révocation doivent être déployés dans un réseau protégé, accessible uniquement aux administrateurs de la TOE ;

- l'administrateur de la base de données doit être considéré comme un administrateur de la TOE.

## 3.3. Reconnaissance du certificat

### *3.3.1. Reconnaissance européenne (SOG-IS)*

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E3 Elémentaire et CC EAL4. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :




### *3.3.2. Reconnaissance internationale critères communs (CCRA)*

Ce certificat est émis dans les conditions de l'accord du CCRA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs. La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :



[1] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.
[2] Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

# Annexe 1. Niveau d'évaluation du produit

| Classe | Famille | Composants par niveau d'assurance | | | | | | | Niveau d'assurance retenu pour le produit | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | EAL 1 | EAL 2 | EAL 3 | EAL 4 | EAL 5 | EAL 6 | EAL 7 | EAL 3+ | Intitulé du composant |
| ADV Développement | ADV_ARC | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Security architecture description |
| | ADV_FSP | 1 | 2 | 3 | 4 | 5 | 5 | 6 | 3 | Functional specification with complete summary |
| | ADV_IMP | | | | 1 | 1 | 2 | 2 | | |
| | ADV_INT | | | | | 2 | 3 | 3 | | |
| | ADV_SPM | | | | | | 1 | 1 | | |
| | ADV_TDS | | 1 | 2 | 3 | 4 | 5 | 6 | 2 | Architectural design |
| AGD Guides d'utilisation | AGD_OPE | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Operational user guidance |
| | AGD_PRE | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Preparative procedures |
| ALC Support au cycle de vie | ALC_CMC | 1 | 2 | 3 | 4 | 4 | 5 | 5 | 3 | Authorisation controls |
| | ALC_CMS | 1 | 2 | 3 | 4 | 5 | 5 | 5 | 3 | Implementation representation CM coverage |
| | ALC_DEL | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Delivery procedures |
| | ALC_DVS | | | 1 | 1 | 1 | 2 | 2 | 1 | Identification of security measures |
| | ALC_FLR | | | | | | | | 3 | Systematic flaw remediation |
| | ALC_LCD | | | 1 | 1 | 1 | 1 | 2 | 1 | Developer defined life-cycle model |
| | ALC_TAT | | | | 1 | 2 | 3 | 3 | | |
| ASE Evaluation de la cible de sécurité | ASE_CCL | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Conformance claims |
| | ASE_ECD | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Extended components definition |
| | ASE_INT | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | ST introduction |
| | ASE_OBJ | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | Security objectives |
| | ASE_REQ | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | Derived security requirements |
| | ASE_SPD | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Security problem definition |
| | ASE_TSS | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | TOE summary specification |
| ATE Tests | ATE_COV | | 1 | 2 | 2 | 2 | 3 | 3 | 2 | Analysis of coverage |
| | ATE_DPT | | | 1 | 2 | 3 | 3 | 4 | 1 | Testing: basic design |
| | ATE_FUN | | 1 | 1 | 1 | 1 | 2 | 2 | 1 | Functional testing |
| | ATE_IND | 1 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | Independent testing: sample |
| AVA Estimation des vulnérabilités | AVA_VAN | 1 | 2 | 2 | 3 | 4 | 5 | 5 | 2 | Vulnerability analysis |

# Annexe 2. Références documentaires du produit évalué

| | |
|---|---|
| [ST] | Cible de sécurité de référence pour l'évaluation :<br>- Cible de sécurité TrustyTime V2<br>Référence : CSSI/HLS/TRUSTY/FR/07/0059, version 1.10 du 01/04/2011<br>C.S. |
| [RTE] | Rapport technique d'évaluation – Projet AMATERASU<br>Référence : OPPIDA/CESTI/ AMATERASU /RTE/1.2 du 31/05/2011<br>OPPIDA |
| [CONF] | Liste de configuration :<br>- TrustyTime – Liste de configuration<br>Référence : CSSI/HLS/TRUSTY/FR/10/0074, version 4.0 du 04/04/2011<br>C.S. |
| [GUIDES] | Guide d'administration du produit :<br>- TrustyTime Manuel d'Administration<br>Référence : CSSI/HLS/TRUSTY/FR/8/0145, version 3.3 du 08/03/2011<br>C.S.<br><br>Guides d'utilisation du produit :<br>- Manuel d'utilisateur – Timestamp Client<br>Référence : CSSI/HLS/TRUSTY/FR/9/0104, version 1.2 du 04/10/2010<br>C.S.<br>- Manuel d'utilisateur – Wizard Configuration<br>Référence : CSSI/HLS/TRUSTY/FR/9/0108, version 1.1 du 04/10/2010<br>C.S.<br>- Manuel d'utilisateur – Assistant context d'horodatage<br>Référence : CSSI/HLS/TRUSTY/FR/10/0059, version 1.0 du 04/10/2010<br>C.S. |

# Annexe 3. Références liées à la certification

| | |
|---|---|
| Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information. | |
| [CER/P/01] | Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, DCSSI. |
| [CC] | Common Criteria for Information Technology Security Evaluation :<br>Part 1: Introduction and general model,<br>September 2006, version 3.1, revision 1, ref CCMB-2006-09-001;<br>Part 2: Security functional components,<br>September 2007, version 3.1, revision 2, ref CCMB-2007-09-002;<br>Part 3: Security assurance components,<br>September 2007, version 3.1, revision 2, ref CCMB-2007-09-003. |
| [CEM] | Common Methodology for Information Technology Security Evaluation :<br>Evaluation Methodology,<br>September 2007, version 3.1, révision 2, ref CCMB-2007-09-004. |
| [CC RA] | Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000. |
| [SOG-IS] | « Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 Janvier 2010, Management Committee. |
| [REF-CRY] | Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr |
| [REF-KEY] | Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 1.10 du 24 octobre 2008 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr |
| [REF-AUT] | Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr |